REMARKS

Upon entry of this Amendment, claims 3-95 are pending. Claims 3-87 stand rejected under 35 U.S.C. § 103(a) as obvious in light of U.S. Patent No. 6,385,596 to *Wiser* in view of U.S. Patents 6,112,304 to *Clawson* and 4,727,243 to *Savar*. New claims 88-95 are presented. Support for the new claims may be found in the originally filed specification, drawing, and claims. The claims as amended traverse the Examiner's rejections. No new matter is submitted.

The Examiner has supported rejection using the terminology "reads on" to link a limitation recited in a claim to a passage of a reference. The terminology is understood to mean that the reference is within the scope of the limitation as opposed to that the reference would have made the limitation obvious.

Rejections Under 35 U.S.C. § 103

Independent claims 3, 25, 47, 66, and 76 were amended February 15, 2004 to include reconciliation. At that time claims 86 and 87 were added as copies of claims 3 and 25 prior to that amendment. Applicant now amends claims 3, 25, 47, 66, and 76 to remove reconciliation and presents claims 86 and 87 amended to include reconciliation.

The Examiner has taken the position in the Office Action mailed that a proposed modification of the system of *Wiser* to include a standard firewall as taught by *Clawson* would have made obvious the methods and systems now recited in claims 3, 25, 47, 66, and 76. Applicant herein proves such a rejection would be improper by showing that several limitations of the claims as amended are absent from the proposed system. When any one limitation is wholly absent from the combination of references cited by the Examiner, a *prima facia* case for rejection for obviousness has not been made and the rejection cannot stand. Further, Applicant shows there is no suggestion to perform the modification because a person of ordinary skill in the art would be motivated to avoid the modification proposed by the Examiner since the modification, instead of providing a benefit of reliability, actually decreases reliability (i.e., causes new problems) as taught by other art of record.

The Examiner has taken the position in the Office Action mailed that a proposed modification of the system of *Wiser* to include a standard firewall as taught by *Clawson* and further modified to include reconciliation as taught by *Savar* would have made obvious the methods and systems now recited in claims 86 and 87. Applicant herein proves such a rejection

would be improper by showing that several limitations of the claims as amended are absent from the proposed system. As mentioned above, a *prima facia* case for rejection for obviousness cannot then stand.

Transfers

Independent claims 3, 25, and 47 variously recite at least one limitation wholly absent from a modification of *Wiser* to include a standard firewall of *Clawson*: "each protected transfer comprises a step for receiving a respective request and a step for delivering per the request, receiving being performed by a respective receiving system linked by a respective network link to a respective delivering system, receiving being performed independently of the delivering system, delivering being performed by the respective delivering system in response to, and otherwise independently of, the receiving system and without identifying the delivering system".

In *Wiser*, the consumer obtains a voucher from the content manager by communicating through the HTTP server to the content manager; the voucher is returned on the same path, to wit, from the content manager through the HTTP server to the consumer. The transfers in *Wiser* are of the type A to B to C (for the request) and C to B to A (for the delivery). The Examiner proposes a standard firewall as taught by *Clawson* and *Shuba* be introduced on a link to isolate the end points of the link. In other words, a standard firewall is a server between A and C or firewall functions added to the HTTP server (B) that already stands between A and C.

In contrast, Applicant solves a problem not recognized in the art. Applicant claims, *inter alia*, communication to obtain a permit of the type A to B (receiving the request), B to C (a network link), and C to A (delivering the permit) (see also new claims 88, 89, 90, and 93). *Wiser* and *Shoen* leave the delivery server open to attack by failing to keep from disclosing the identity of the delivery server from the consumer. *Wiser* is inoperative without disclosing the identity of the delivery server to the consumer because the consumer uses the identity in the voucher to request delivery directly from the delivery server. Assuming, *arguendo*, that suggestion could be found for adding a standard firewall on the delivery link in *Wiser* or *Shoen*, such a configuration would exhibit decreased delivery speed and lower reliability as it includes a bottleneck through the standard firewall. Applicant protects the delivery server from attack without using a standard firewall. No art of record teaches or suggests communication of the type recited in the claim in combination with the limitation "without identifying the delivering system".

Independent claim 66 recites at least one limitation wholly absent from a modification of *Wiser* to include a standard firewall of *Clawson*: "a first port that conducts a first transaction with the client port to establish a request for a permit and that conducts a second transaction with the client port to establish a request for a data product". In *Wiser*, the request for a voucher goes to the HTTP server; and, the request for the product goes to the delivery server. Assuming, *arguendo*, that suggestion could be found for adding a standard firewall to *Wiser*, adding the teachings of a standard firewall would not change the functions of the HTTP server or delivery server in *Wiser* nor the paths of communication to meet the recited claim limitation. Consequently, the proposed modification of *Wiser* does not include at least the limitation of claim 66 quoted above. No art of record suggests this limitation nor would have made it obvious.

Independent claim 76 recites at least one limitation wholly absent from a modification of *Wiser* to include a standard firewall of *Clawson*: "a first interface that accesses a request for a permit, the request for a permit originating on the client, and that accesses a request for a data product, the request for a data product originating on the client and including at least a portion of a permit;" and "a second interface that provides access to the permit across the second interface to the client" wherein the second interface is distinct from the first interface. As discussed above, access to the voucher in *Wiser* is provided through an interface (of the HTTP server); but this interface is not an interface "that accesses a request for a permit, ... and that accesses a request for a data product". There is nothing in *Wiser* that corresponds to the "first interface" as claimed. There is nothing in the proposed modification to add the teachings of *Clawson* that supplies this missing limitation nor further supplies the "second interface" as claimed.

In *Wiser*, the IP address of the delivery system is necessarily provided in the voucher. Without the IP address of the delivery system, no delivery of the product can be initiated by the customer. If a firewall operative as a proxy server to mask IP addresses were introduced between the customer and the delivery server (so as to satisfy the limitations of the claim as to delivery of the product), the combination would become inoperative for the intended purpose of delivering the product. *Clawson* only teaches a firewall operative as a proxy server to mask IP addresses. To realize exactly what is taught by *Clawson*, *Clawson* may be understood from other prior art including *Shuba* and a conventional dictionary of computer terminology.

A firewall as described by *Clawson* is a process (there called a denizen) that provides IP masking, IP filtering, and user authentication. The following passages are quoted from *Clawson* to show what *Clawson* teaches.

> Computing processes 100 are viewed as creatures inhabiting an ocean 102 of computing resources residing at various locations 104. A given machine in a network may contain one or more locations 104. An ocean 102 can reside on one machine or several. Likewise, all locations 104 can be viewed as belonging to a single operational environment 102, or they can be grouped into separate connectable oceans 102. ... The "denizen" processes 100, also known as "Organic Data Elements" or "OEDs" ... can move along paths 106 between locations 104 in the computational "ocean" that serves as their operational environment 102. (col. 7 lines 1-14).
>
> In one embodiment, the river pod denizen 814 is also parent to a gatekeeper ODE 818. The gatekeeper 818 has two main functions. The first is security; the gatekeeper 818 provides the capabilities of standard firewall systems such as IP masking, IP filtering, and user authentication. (Col. 18 lines 33-37).

A person of ordinary skill would understand the phrase "standard firewall" as referred to in *Clawson* to be a firewall of the type described in "A Reference Model for Firewall Technology" by *Shuba* quoted in pertinent part below.

> Classically, firewall technology has been applied to TCP/IP (transmission control protocol, internet protocol) internetworks. Firewalls are used to guard and isolate connected segments of internetworks. "Inside" network domains are protected against "outside" untrusted networks, or parts of a network are protected against other parts. Various architectures for firewalls have been

> published and built, such as filtering routers, or application level proxy services. (sec. 1 para. 2). ... Firewall technology is a set of mechanisms that can enforce a network domain security policy on communication traffic entering or leaving a network policy domain. A firewall system, or firewall, is an instantiation of firewall technology. This characterization covers the current state of firewall technology. Furthermore, it includes the view of firewall technology as a distributed security architecture placed on the locally controlled data transmission path between communication endpoints. (sec. 2.1 para. 2). ... [A] reference model [describing an instance of firewall technology] consists of the following functional components: authentication function, integrity function, access control function, audit function, and access enforcement function. (sec. 4 para. 1).

The standard firewall in *Clawson* and *Shuba*, is a computer between a first network (untrusted) and a second network (a protected domain). If this were not so, then the firewall in *Clawson* could not "guard and isolate" as specifically taught in *Shuba* quoted above.

A person of ordinary skill in reading the phrase "IP masking" in *Clawson* would understand that *Clawson* is referring to a firewall (i.e., a computer between two networks) that is functioning as a proxy service between a client on the untrusted network and a server within the network policy domain. The terms "proxy service" and "proxy server" are defined for example in the "Computer Desktop Encyclopedia" version 17.2 by The Computer Language Company, Inc. as follows:

> Proxy server -- Also called a "proxy," it is a computer system or router that breaks the connection between sender and receiver, closing a straight path between the internal LAN and the Internet. Very often the proxy server is a dual-homed host with two network interfaces. Functioning as a relay between the client and server, proxy servers are used to help prevent a cracker from

obtaining internal addresses and attacking the private network. They are one of several tools that can be used to build a firewall.

The word proxy means "to act on behalf of another," and a proxy server acts on behalf of the client and of the server. All requests from the clients to the Internet go to the proxy server first. The proxy evaluates them and passes valid ones on to the Internet. Likewise, responses from the Internet or initial requests coming from the Internet go [to] the proxy and are evaluated, before being passed on to the clients. Proxies generally employ network address translation (NAT), which presents one organization-wide IP address to the outside world. Proxies may also cache Web pages, so that the next client request for that same page can be obtained locally, which is much faster.

Proxy servers are available for common Internet services; for example, an HTTP proxy is used for Web access; an FTP proxy is used for file transfers. Such proxies are called "application-level" proxies or "application-level gateways," because they are dedicated to a particular application and protocol and are aware of the content of the packets being sent. A generic proxy, called a "circuit-level" proxy, supports multiple applications. For example, SOCKS is a generic IP-based proxy server that supports TCP and UDP applications (see SOCKS).

The SMTP mail standard is an example of a proxy server without being called one, because it uses a store-and-forward server. E-mail messages are not sent directly from client to client without going through a mail server. See LAN, firewall, proxy and cache.

Wiser teaches merely communication between two computers for delivery of a voucher and communication between two computers for delivery of a product. Assuming, *arguendo*, that a combination of the teachings of *Wiser* and *Clawson* met the limitations of the independent

claims discussed above (which it plainly does not as also discussed above), there is no suggestion in *Clawson* or any other art of record that would lead to the combination proposed by the Examiner. The suggestion identified by the Examiner is not logically related to the combination and therefore cannot serve as suggestion.

First, the suggestion is not logical because a computer operating as a firewall is serving a different function than the servers on the networks it isolates. A parallel combination of similarly functioning servers for higher reliability as mentioned in *Clawson* does not suggest the addition of a functionally different server for firewall functions. Furthermore, *Shuba* points out that adding a firewall decreases reliability by introducing a choke point, or single point of failure.

> [In the] classical view ... firewalls are security devices that enforce security policy close to the network perimeter. ... The firewall is a central point of failure and becomes a performance bottleneck in the presence of high performance networking technologies. The distribution of [firewall] functions ... reduces the performance overhead experienced at the network perimeter because fewer functions need to be computed there. Functions provided further inside the network can be executed concurrently, thus contributing to an overall performance increase of the distributed firewall. In this fashion, firewall security services can be constructed in an architecture that scales better than previous designs. The distribution of the components may be driven not only by criteria, such as performance increase through replication of functions, but also by the goal to improve reliability, availability, and disaster protection through redundant distribution of functions. Single points of failure can be avoided by design. (sec. 5 para. 2).

In other words, a person of ordinary skill would not be led to add a firewall if seeking to improve the reliability of a distributed processing system.

Second, the passage from *Clawson* quoted by the Examiner is taken out of a context that teaches away from obtaining desired results merely by adding a firewall to a distributed processing system. To avoid the bottleneck and poor reliability taught by *Shuba*, a person following *Shuba* would consider distributing the firewall functions, that is, design a distributed computing environment for firewall functions. *Clawson*, in the same column as the passage quoted by the Examiner, goes on to state:

> As a result, many different approaches to distributed computing have been tried, and even more have been proposed. Each distributed computing system, whether it has been implemented or not, embodies numerous design choices, making it one approach selected from an enormous universe of possibilities. Some of the most important design choices include deciding how the distributed processes communicate with one another and with users, how security constraints are defined and enforced, how and when processors and processes should be brought together and separated, how responsibility is divided between processes, how processes are updated to reflect new data or instructions, and how processes should detect and handle errors. (col. 1 lines 48-60).

Taken in context of the "enormous universe of possibilities", the statement of *Clawson* to "harness the computing power of many connected processors together into one large system" is too vague to constitute suggestion to specifically add a firewall to the system of *Wiser*. Nothing in *Clawson* including the passage quoted by the Examiner teaches or suggests that the firewall teachings of *Clawson* can be combined with the system of *Wiser* as proposed by the Examiner.

Applicant's claimed methods and systems accomplish secure delivery of product without the teachings of a "standard firewall" of *Clawson* or the teachings of distributed firewall functions of *Shuba*. As claimed, the permit is not being delivered through a firewall at least because it does not pass through the same computer that received the request for the permit. As claimed, the product is not being delivered through a firewall at least because it does not pass

through the same computer that received the permit for delivery. Applicant's claimed methods and systems accomplish secure delivery without the expense and bottleneck of a firewall.

As discussed above, the combination proposed by the Examiner does not perform the functions claimed. Further, the suggestion identified by the Examiner is not sufficient to lead a person of ordinary skill to make the proposed combination. Still further, Applicant's claimed invention solves a problem not solved in the prior art. And further still, the claimed invention provides a result different from the combination proposed by the Examiner.

Reconciliation

Independent claims 86 and 87 variously recite at least one limitation wholly absent from a modification of *Wiser* to include a standard firewall of *Clawson* further modified to include the teachings of *Savar*: "a step for receiving a plurality of reports comprising reports transmitted in response to requests for permits and reports transmitted in response to attempted accesses of products; and a step for identifying, as indicated by a set of reports of the plurality, at least one of incomplete transactions and events that indicate unauthorized attempted access, wherein each complete transaction comprises delivery of a product specified in a delivered permit".

In *Savar* there is no "receiving of a plurality of reports" as recited in the claims. Further, there is no "identifying as indicated by a set of reports", as claimed. Still further, there is no "complete transaction [comprising] delivery of a product specified in a delivered permit", as claimed. Reconciliation as taught by *Savar* has as its goal the completing of incomplete transactions so that an accurate sum of transaction values can be prepared. Each transaction in *Savar* includes one request for authorization of an amount to be taken on credit and one response being approval or rejection of the request. A sum of transaction values is to include only those values for transactions wherein the response was approval.

Nowhere in *Savar*, *Wiser*, or *Clawson* is there any mention of "reports comprising reports transmitted in response to requests for permits and reports transmitted in response to attempted accesses of products" as claimed. For lack of such reports, there is furthermore no mention in *Savar*, *Wiser*, or *Clawson* of "identifying, as indicated by a set of reports of the plurality, at least one of incomplete transactions and events that indicate unauthorized attempted access, wherein each complete transaction comprises delivery of a product specified in a delivered permit".

If it is argued that the approval of credit is itself a report in *Savar* then there is nothing corresponding to the product or to another type of report so as to have a set of reports describing one transaction.

The differences between a transaction in *Savar* and a transaction as claimed are not suggested by any art of record. For example, as claimed, a transaction includes a permit and a product specified in the permit. There is no product in *Savar*. The request for credit approval in *Savar* is not a request specifying a product to be delivered. There is no access to a product in *Savar*. There is no attempted access to a product in *Savar*.

Applicant's claimed invention is not obvious in light of the proposed combination of *Wiser*, *Clawson*, and *Savar*, *inter alia*, because the claimed invention provides a different result than the combination proposed by the Examiner. The combination of teachings proposed by the Examiner does not solve problems solved by Applicant, including, being able to identify unauthorized attempted access. In a system using the teachings of *Savar* nothing is derived from incomplete transactions, which are assumed to be discarded. The value of an incomplete transaction in *Savar* is not part of the sum which is the result of reconciliation. As such, *Savar*, teaches away from deriving valuable information from incomplete transactions, such as tracking of unauthorized attempted access.

As discussed above, the combination proposed by the Examiner does not include all limitations of the claim. Because structures and functions recited in amended claim 86 and 87 are not made obvious from the combination of *Wiser*, *Clawson*, and *Savar*, (in part because some structures and functions are entirely absent from this combination), amended claims 86 and 87 are in condition for allowance.

Conclusion

The application is believed to be in condition for allowance and favorable action is respectfully requested. The Examiner is invited to telephone the undersigned at the telephone number listed below if it would in any way advance prosecution of this case.

While no fees are believed due, Applicants hereby request that any other required fee to maintain pendency of this case, except for the Issue Fee, be charged to Deposit Account No. 13-0762.

Respectfully submitted,
MACROVISION CORPORATION

Date: 4/28, 2005

James H. Salter (Reg. No. 35,668)

2830 De La Cruz Boulevard
Santa Clara, CA 95050
Tel: (408) 562-8400
Fax: (408) 567-1800

FIRST CLASS CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 29, 2005.

Barbara Skliba
Name of Person Mailing Correspondence

Barbara Skliba — 4/29/05
Signature — Date